

# REȚELE DE CALCULATOARE

Tema 1. Descrierea topologiilor rețelelor de date .....	2
Fișa suport 1.1. Transmisia datelor în rețelele de calculatoare .....	2
Fișa suport 1.2. Tipuri de rețele.....	4
Fișa suport 1.3. Topologii.....	7
Tema 2 Arhitectura rețelelor de calculatoare .....	9
Fisa suport Arhitectura Ethernet, Token-Ring, FDDI.....	9
Tema 3 Standarde Ethernet.....	11
Fișa suport Standarde pentru rețele Ethernet.....	11
Tema 4 Modele de date .....	12
Fișa suport Modelul OSI și TCP/IP.....	12
Tema 5 Adresarea IP.....	16
Fisa suport 5.1 Structura unei adrese IP .....	16
Fisa suport 5.2. Clase de adrese IP .....	17
Fisa suport 5.3 Adresarea IP în subrețele .....	18
Tema 6 Serviciul de rezolvare a numelui .....	20
Fișa suport Descrierea serviciului DNS .....	20
Tema 7 Suita de protocoale TCP/IP .....	21
Fișa suport Protocoale TCP/IP .....	21

## Tema 1. Descrierea topologiilor rețelelor de date

### Fișa suport 1.1. Transmisia datelor în rețelele de calculatoare



O rețea de calculatoare este alcătuită dintr-un ansamblu de echipamente interconectate între ele prin intermediul unor echipamente de rețea, cu scopul transmisiei de date și partajării resurselor.



Fig.1.1 Resurse în rețele de calculatoare

O rețea poate partaja diverse tipuri de resurse:

- *Servicii* – cum ar fi imprimarea sau scanarea
- *Spații de stocare pe suporturi externe* – cum ar fi hard-diskurile
- *Aplicații* – cum ar fi bazele de date

Echipamentele interconectate pot fi *sisteme de calcul* (desktop sau laptop) sau *echipamente periferice* (imprimante, scannere etc)

Conectivitatea este asigurată de echipamente de rețea (hub-uri, switch-uri, rutere, puncte de acces wireless)

Transmisia datelor se realizează prin medii de transmisie care pot fi:

- *Conductoare de cupru* – pentru transmisia datelor sub formă de semnale electrice
- *Fibră optică* – din fibre de sticlă sau materiale plastice – pentru a transporta datele sub formă de impulsuri luminoase
- *Medii de transmisie a datelor fără fir* – transmit datele sub formă de unde radio, microunde, raze infraroșii sau raze laser - în cadrul conexiunilor fără fir (wireless)

În timpul transmisiei de la un calculator sursă la un calculator destinație, datele suferă o serie de modificări:

Înainte de a fi transmise în rețea, datele sunt transformate în flux de caractere alfanumerice, apoi sunt împărțite în segmente, care sunt mai ușor de manevrat și permit mai multor utilizatori să transmită simultan date în rețea.

Fiecărui segment i se atașează apoi un antet (header), care conține o serie de informații suplimentare cum ar fi: un semnal de atenționare, care indică faptul că se transmite un pachet de date; adresa IP a calculatorului-sursă; adresa IP a calculatorului-destinație; informații de ceas pentru sincronizarea transmisiei) și un postambul care este de obicei o componentă de verificare a erorilor(CRC). Segmentul, astfel modificat se numește pachet, pachet IP sau datagramă

Fiecărui pachet i se atașează apoi un al doilea antet care conține adresele MAC ale calculatorului-sursă, respectiv ale calculatorului-destinație. Pachetul se transformă astfel în cadru (frame)

START	ADRESĂ	TIP/LUNGIME	DATE	CRC	STOP
-------	--------	-------------	------	-----	------

Fig. 1.2. Structura generală a unui cadru

Cadrele circulă prin mediul de transmisie sub formă de șiruri de biți. Există mai multe tipuri de cadre, în funcție de standardele folosite la descrierea lor (cadru Ethernet, cadru FDDI, etc.)

Odată ajunse la calculatorul-destinație, șirurile de biți suferă procesul invers de transformare. Li se detașează antetele, segmentele sunt apoi reasamblate, li se verifică integritatea și numărul, apoi sunt aduse la o formă care poate fi citită de utilizator.

Procesul de împachetare a datelor se numește încapsulare, iar procesul invers, de detașare a informațiilor suplimentare se numește decapsulare. Trebuie menționat că în timpul încapsulării, datele propriu-zise rămân intacte.

Sunt definite două tehnologii de transmisie a datelor:

- transmisia prin difuzare (broadcast);
- transmisia punct-la-punct;

*Transmisia prin difuzare* utilizează de cele mai multe ori un singur canal de comunicație care este partajat de toate stațiile din rețea. Orice stație poate trimite pachete, care sunt primite de toate celelalte stații, operațiunea numindu-se difuzare. Stațiile prelucrează numai pachetele care le sunt adresate și le ignoră pe toate celelalte. În unele rețele cu difuzare este posibilă transmisia simultană de pachete către mai multe stații conectate la rețea, operațiune ce poartă numele de trimitere multiplă. Această tehnică se utilizează cu precădere în rețelele de mici dimensiuni, localizate în aceeași arie geografică

*Transmisia punct-la-punct* se bazează pe conexiuni pereche între stații, cu scopul transmiterii de pachete. Pentru a parcurge traseul de la o sursă la destinație într-o rețea de acest tip, un pachet va „calatori” prin una sau mai multe mașini intermediare. Pot exista mai multe trasee între o sursă și o destinație motiv pentru care în aceste situații este necesară implementarea unor algoritmi specializați de dirijare. Tehnica punct-la-punct este caracteristică rețelelor mari.



Cantitatea de informație care poate fi transmisă în unitatea de timp este exprimată de o mărime numită *lățime de bandă* (bandwidth), și se măsoară în biți pe secundă (bps). Adeseori în aprecierea lățimii de bandă se folosesc multiplii cum ar fi:

Kbps – kilobiți pe secundă

Mbps – megabiți pe secundă

O rețea suportă trei moduri de transmisie a datelor: simplex, half-duplex și full-duplex

- *Simplex*- întâlnit și sub numele de transmisie unidirecțională, constă în transmisia datelor într-un singur sens. Cel mai popular exemplu de transmisie simplex este transmisia semnalului de la un emițător (stația TV) către un receptor (televizor)
- *Half-duplex* – constă în transmiterea datelor în ambele direcții alternativ. Datele circulă în acest caz pe rând într-o anumită direcție. Un exemplu de transmisie half-duplex este transmisia datelor între stațiile radio de emisie-recepție. Sistemele sunt formate din două sau mai multe stații de emisie-recepție dintre care una singură joacă rol de emițător, în timp ce celelalte joacă rol de receptor
- *Full-duplex* – constă în transmisia datelor simultan în ambele sensuri. Lățimea de bandă este măsurată numai într-o singură direcție (un cablu de rețea care funcționează în full-duplex la o viteză de 100 Mbps are o lățime de bandă de 100 Mbps). Un exemplu de transmisie full-duplex este conversația telefonică.

## Fișa suport 1.2. Tipuri de rețele

O clasificare a rețelelor după criteriul răspândirii pe arii geografice, al modului de administrare și al mediului de transmisie a datelor ar evidenția, printre altele, următoarele trei tipuri de rețele, frecvent întâlnite în documentație:

- Rețele locale de calculatoare (LAN – Local Area Network)
- Rețele de întindere mare (WAN – Wide Area Network)
- Rețele fără fir (WLAN – Wireless Local Area Network)

### Rețele locale de calculatoare



Fig. 1.3 Rețea locală de calculatoare

Rețeaua locală de calculatoare este o rețea de echipamente interconectate răspândite pe o suprafață de mici dimensiuni (încăpere, clădire, grup de clădiri apropiate).

Conform unor surse, conceptul de LAN face referire la o rețea de calculatoare interconectate și supuse aceluiași politici de securitate și control a accesului la date, chiar dacă acestea sunt amplasate în locații diferite (clădiri sau chiar zone geografice). În acest context, conceptul de local se referă mai degrabă la controlul local decât la apropierea fizică între echipamente. Transmisia datelor în rețelele LAN tradiționale se face prin conductoare de cupru.

#### Rețelele de întindere mare

O rețea de întindere mare este alcătuită din mai multe rețele locale (LAN-uri) aflate în zone geografice diferite. Rețelele de întindere mare acoperă arii geografice extinse, o rețea WAN se poate întinde la nivel național sau internațional.

În mod specific în aceste rețele calculatoare se numesc gazde (host), termen care se extinde și la rețelele LAN care fac parte din acestea. Gazdele sunt conectate printr-o subrețea de comunicație care are sarcina de a transporta mesajele de la o gazdă la alta. Subrețeaua este formată din două componente distincte: liniile de transmisie și elementele de comutare. Elementele de comutare, numite generic noduri de comutare, sunt echipamente specializate, folosite pentru a interconecta două sau mai multe linii de transmisie.

Unele rețele WAN aparțin unor organizații a căror activitate se desfășoară pe o arie largă și sunt private. Cel mai popular exemplu de rețea WAN este Internetul, care este format din milioane de LAN-uri interconectate cu sprijinul furnizorilor de servicii de comunicații (TSP-Telecommunications Service Providers).

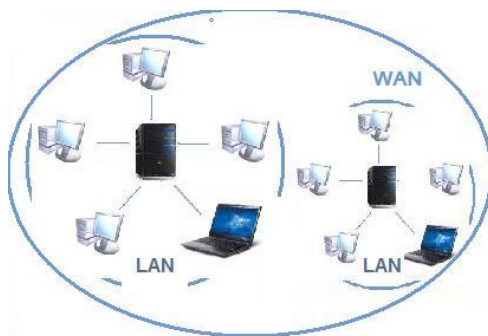


Fig.1.4. Rețea de întindere mare

### Rețele fără fir

Sunt rețele locale care transmit datelor se face prin medii fără fir. Într-un WLAN, stațiile, care pot fi echipamente mobile – laptop – sau fixe – desktop – se conectează la echipamente specifice numite puncte de acces. Stațiile sunt dotate cu plăci de rețea wireless. Punctele de acces, de regulă routere, transmit și recepționează semnale radio către și dinspre dispozitivele wireless ale stațiilor conectate la rețea.



Punctele de acces se conectează de obicei la rețeaua WAN folosind conductoare de cupru. Calculatoarele care fac parte din WLAN trebuie să se găsească în raza de acțiune a acestor puncte de acces, care variază de la valori de maxim 30 m în interior la valori mult mai mari în exterior, în funcție de tehnologia utilizată.

Primele transmisii de date experimentale în rețele wireless au avut loc în anii 70 și au folosit ca agent de transmisie a datelor în rețea unde radio sau razele infraroșii. Între timp, tehnologia a evoluat și s-a extins până la nivelul utilizatorilor casnici.

În prezent există mai multe moduri de a capta datele din eter: Wi-Fi, Bluetooth, GPRS, 3G ș.a. Acestea li se adaugă o nouă tehnologie care poate capta datele de șapte ori mai repede și de o mie de ori mai departe decât populara tehnologie Wireless Fidelity (Wi-Fi), numită WiMAX. În timp ce rețelele Wi-Fi simple au o rază de acțiune de aproximativ 30 m, WiMax utilizează o tehnologie de microunde radio care mărește distanța la aproximativ 50 km. Astfel, se pot construi rețele metropolitane WiMAX.

Avantaje:

- Simplitate în instalare.
- Grad ridicat de mobilitate a echipamentelor – tehnologia s-a popularizat cu precădere pentru conectarea la rețea a echipamentelor mobile
- Tehnologia poate fi utilizată în locații în care cablarea este dificil sau imposibil de realizat
- Costul mai ridicat al echipamentelor wireless este nesemnificativ raportat la costul efectiv și costul manoperei în cazul rețelelor cablate
- Conectarea unui nou client la o rețea wireless nu implică folosirea unor echipamente suplimentare

Dezavantaje

- Securitate scăzută
- Raza de acțiune în cazul folosirii echipamentelor standard este de ordinul zecilor de metri. Pentru extinderea ei sunt necesare echipamente suplimentare care cresc costul
- Semnalele transmise sunt supuse unor fenomene de interferențe care nu pot fi controlate de administratorul de rețea și care afectează stabilitatea și fiabilitatea rețelei – motiv pentru care serverele sunt rareori conectate wireless
- Lățimea de bandă mică (1-108 Mbit/s) în comparație cu cazul rețelelor cablate (până la câțiva Gbit/s)



Fig 1.5. Rețea LAN fără fir

### Rețele peer-to-peer (P2P) vs rețele client-server

Într-o rețea de calculatoare comunicarea are loc între două entități: *clientul* care emite o cerere prin care solicită o anumită informație și *serverul* care primește cererea, o prelucrează iar apoi trimite clientului informația solicitată. Dacă ar fi să clasificăm rețelele după ierarhia pe care o au într-o rețea echipamentele conectate, ar trebui să facem referire la două tipuri de rețele:

- Rețele de tip peer-to-peer
- Rețele de tip client-server

Într-o rețea *peer-to-peer*, toate calculatoarele sunt considerate egale (peers), fiecare calculator îndeplinește simultan și rolul de client și rolul de server, neexistând un administrator responsabil pentru întreaga rețea. Un exemplu de serviciu care poate fi oferit de acest tip de rețele este partajarea fișierelor. Acest tip de rețele sunt o alegere bună pentru mediile în care: există cel mult 10 utilizatori, utilizatorii se află într-o zonă restrânsă, securitatea nu este o problemă esențială, organizația și rețeaua nu au o creștere previzibilă în viitorul apropiat

Neajunsuri ale rețelelor peer-to-peer:

- Nu pot fi administrate centralizat
- Nu poate fi asigurată o securitate centralizată, ceea ce înseamnă că fiecare calculator trebuie să folosească măsuri proprii de securitate a datelor

- Datele nu pot fi stocate centralizat, trebuie menținute backup-uri separate ale datelor, iar responsabilitatea cade în sarcina utilizatorilor individuali.
- Administrarea rețelelor peer-to-peer este cu atât mai complicată cu cât numărul calculatoarelor interconectate este mai mare

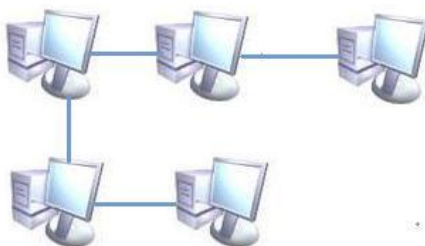


Fig.1.6.Rețea peer-to-peer

Rețele *client-server*, în care un calculator îndeplinește rolul de server, în timp ce toate celelalte îndeplinesc rolul de client. De regulă, serverele sunt specializate (servere dedicate) în efectuarea diferitelor procesări pentru sistemele-client, cum ar fi:

- Servere de fișiere și imprimare – oferă suport sigur pentru toate datele și gestionează tipărirea la imprimantele partajate în rețea
- Servere web – găzduiesc pagini web
- Servere pentru aplicații – cum ar fi serverele pentru baze de date
- Servere de mail – gestionează mesaje electronice
- Servere pentru gestiunea securității – asigură securitatea unei rețele locale când aceasta este conectată la o rețea de tipul Internetului – exemple: firewall, proxy-server
- Servere pentru comunicații – asigură schimbul de informații între rețea și clienții din afara acesteia

Rețelele client-server se folosesc cu precădere pentru comunicarea de date în rețea, marea majoritate a aplicațiilor software dezvoltate au la bază acest model. Printre avantajele rețelelor de tip client-server se numără: administrarea centralizată, administratorul de rețea fiind cel asigură back-up-urile de date, implementează măsurile de securitate și controlează accesul utilizatorilor la resurse, funcționarea cu sisteme-client de capacități diverse, securitate ridicată a datelor, controlul accesului exclusiv la resurse a clienților autorizați, întreținere ușoară

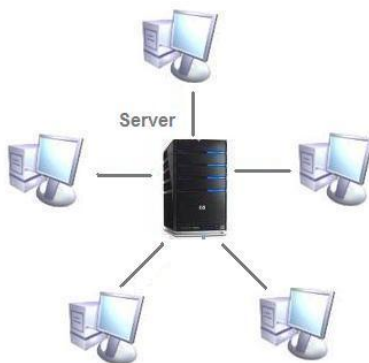


Fig.1.7 Rețea client-server

Rețelele hibride – sunt o combinație a modelului client-server cu modelul peer-to-peer. Stațiile (peers) depozitează resursele partajate iar serverul păstrează informații în legătură cu stațiile ( adresa lor, lista resurselor deținute de acestea) și răspunde la cererea de astfel de informații. Un exemplu de serviciu oferit de o astfel de rețea este descărcarea de fișiere de pe site-urile torrent.

## Fișa suport 1.3. Topologii

Topologia este un termen care desemnează maniera de proiectare a unei rețele. Există două tipuri de topologii: topologia fizică și topologia logică



Topologia logică descrie metoda folosită pentru transferul informațiilor de la un calculator la altul.

Cele mai comune două tipuri de topologii logice sunt *broadcast* și *pasarea jetonului (token passing)*

Într-o topologie broadcast, o stație poate trimite pachete de date în rețea atunci când rețeaua este liberă (prin ea nu circulă alte pachete de date). În caz contrar, stația care dorește să transmită așteaptă până rețeaua devine liberă. Dacă mai multe stații încep să emită simultan pachete de date în rețea, apare fenomenul de coliziune. După apariția coliziunii, fiecare stație așteaptă un timp (de durată aleatoare), după care începe din nou să trimită pachete de date. Numărul coliziunilor într-o rețea crește substanțial odată cu numărul de stații de lucru din rețeaua respectivă, și conduce la încetinirea proceselor de transmisie a datelor în rețea, iar dacă traficul depășește 60% din lățimea de bandă, rețeaua este supraîncărcată și poate intra în colaps.

*Pasarea jetonului* controlează accesul la rețea prin pasarea unui jeton digital secvențial de la o stație la alta. Când o stație primește jetonul, poate trimite date în rețea. Dacă stația nu are date de trimis, pasează mai departe jetonul următoarei stații și procesul se repetă.



Topologia fizică definește modul în care calculatoarele, imprimantele și celelalte echipamente se conectează la rețea.

Topologii fizice fundamentale sunt : magistrală, inel, stea, plasă (mesh), arbore

### Topologia magistrală



Folosește un cablu de conexiune principal, la care sunt conectate toate calculatoarele. Cablul principal are la capete instalate capace (terminatoare) care previn fenomenul de reflexie a semnalelor, fenomen care poate genera erori în transmisia datelor.

Topologia magistrală are avantajul consumului redus de cablu și al conectării facile a calculatoarelor. În schimb, identificarea defectelor de rețea este dificilă, dacă apar întreruperi în cablu, rețeaua nu mai funcționează și este nevoie de terminatori la ambele capete ale cablului

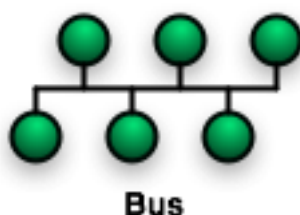


Fig.1.8. Topologia magistrală

### Topologia inel



Într-o topologie inel (ring), fiecare dispozitiv este conectat la următorul, de la primul până la ultimul, ca într-un lanț

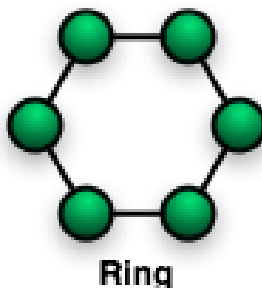


Fig.1.9. Topologia inel

### Topologia stea



Are un punct de conectare central, care este de obicei un echipament de rețea, precum un hub, switch sau router. Fiecare stație din rețea se conectează la punctul central prin câte un segment de cablu, fapt care conferă acestei topologii avantajul că se depanează ușor. Dacă un segment de cablu se defectează, acest defect afectează numai calculatorul la care este conectat, celelalte stații rămânând operaționale.

Topologia stea are dezavantajul costului ridicat și al consumului ridicat de cablu. În plus, dacă un hub se defectează, toate echipamentele din acel nod devin nefuncționale. În schimb, calculatoarele se



conectează ușor, rețeaua nu este afectată dacă sunt adăugate sau deconectate calculatoare și detectarea defectelor este simplă



**Star**

Fig.1.10. Topologia stea



### **Topologia plasă (mesh)**

Într-o topologie mesh, fiecare echipament are conexiune directă cu toate celelalte. Dacă unul din cabluri este defect, acest defect nu afectează toată rețeaua ci doar conexiunea dintre cele două stații pe care le conectează. Altfel spus, dacă o parte a infrastructurii de comunicație sau a nodurilor devine nefuncțională, se găsește oricând o nouă cale de comunicare.

Topologia plasă se folosește în cadrul rețelelor WAN care interconectează LAN-uri. În plus, datorită fiabilității ridicate aceste topologii sunt exploatate în cazul aplicațiilor spațiale, militare sau medicale unde întreruperea comunicației este inacceptabilă



**Fully Connected**

Fig.1.11. Topologia plasă



### **Topologia arbore (tree)**

Combină caracteristicile topologiilor magistrală și stea. Nodurile sunt grupate în mai multe topologii stea, care, la rândul lor, sunt legate la un cablu central.

Topologia arbore prezintă dezavantajul limitării lungimii maxime a unui segment. În plus, dacă apar probleme pe conexiunea principală sunt afectate toate calculatoarele de pe acel segment. Avantajul topologiei arbore constă în faptul că segmentele individuale au legături directe



**Tree**

Fig.1.12. Topologia arbore

În practică se întâlnesc de multe ori topologii compuse rezultate din combinarea topologiilor fundamentale, cum ar fi, spre exemplu este topologia magistrală-stea: mai multe rețele cu topologie stea sunt conectate la un cablu de conexiune principal.



## Tema 2 Arhitectura rețelelor de calculatoare

### Fisa suport Arhitectura Ethernet, Token-Ring, FDDI

Arhitecturile pentru LAN descriu atât topologiile fizice cât și pe cele logice folosite într-o rețea


#### Arhitectura Ethernet


**Ethernet** este denumirea unei familii de tehnologii de rețele de calculatoare, bazate pe transmisia cadrelor (frames) și utilizate la implementarea rețelelor locale de tip LAN. Ethernetul se definește printr-un șir de standarde pentru cablare și semnalizare aparținând primelor două nivele din Modelul de Referință OSI - nivelul fizic și legătură de date.

Numele ethernet provine de la cuvântul "eter" ilustrând faptul că mediul fizic (de exemplu cablurile) transportă biți către toate stațiile de lucru într-un mod asemănător cu străvechiul "luminiferous ether", despre care se credea odată că este mediul prin care se propagă undele electromagnetice<sup>1</sup>


Ethernetul a fost inventat pe baza ideii că pentru a lega computerele între ele astfel ca să formeze o rețea este nevoie de un mediu de transmisie central cum ar fi un cablu coaxial partajat. Conceptul și implementarea Ethernetului s-au dezvoltat permanent, ajungându-se azi la tehnologiile de rețea complexe, care constituie fundamentul majorității LAN-urilor actuale. În loc de un mediu (cablu) central, tehnologiile moderne utilizează legături de tipul punct-la-punct, hub, switch (română comutator), bridge (română punte) și repeater, bazate pe fire de cupru torsadate care reduc costurile instalării, măresc fiabilitatea și înlesnesc managementul și reparațiile rețelei.


Arhitectura Ethernet folosește:

 o topologie logică de tip broadcast și o topologie fizică de tip magistrală sau stea. Vitezele de transfer standard sunt de 10 Mbps și 100 Mbps, iar noile standarde specifice pentru arhitectura Gigabit Ethernet permit viteze de până la 1000 Mbps.

 metoda de control a accesului CSMA/CD (Carrier Sense Multiple Access Collision Detection = Acces multiplu cu detecția purtătoarei și coliziunii). Conform acestei metode, dacă o stație din rețea dorește să transmită date trebuie ca înainte să "asculte"

mediul de transmisie, proces similar cu a aștepta tonul înainte de a forma un număr pe linia telefonică. Dacă nu detectează nici un alt semnal, atunci poate să trimită datele. Dacă nici una din celelalte stații conectate la rețea nu transmite date în acel moment, datele transmise vor ajunge în siguranță la calculatorul destinație, fără nici o problemă. Dacă, însă, în același moment cu primul calculator, și alt calculator din rețea decide că mediul de transmisie este liber și transmite datele în același moment cu primul, va avea loc o coliziune. Prima stație din rețea care a depistat coliziunea, adică dublarea tensiunii pe mediul de transmisie, va transmite către toate stațiile un semnal de jam, care le avertizează să oprească transmisia și să execute un algoritm de încetare a comunicației pentru un timp (backoff algorithm). Acest algoritm generează un timp aleator de una, două milisecunde sau chiar mai scurt, de circa o miime de secundă, interval de timp după care stațiile să reînceapă transmisia. Algoritmul este repetat ori de câte ori apare o coliziune în rețea.

 cablu coaxial ( la primele rețele Ethernet) torsadat sau fibre optice ca mediu de transmisie a datelor

 al cadrul Ethernet, ce constă dintr-un set standardizat de biți utilizat la transportul datelor și cărui structură este ilustrată mai jos:

PRE	START	A D	A S	TIP/LUNGIME	DATE	CRC
7 byte	1 byte	6 byte	6 byte	4 byte	46-1500 byte	4 byte

Fig.2.1. Structura unui cadru Ethernet

- PRE - Preambulul constă într-o secvență alternantă de 1 și 0 ce indică stațiilor receptoare sosirea unui cadru
- START - Delimitatorul de start al cadrului - conține o secvență alternantă de 1 și 0 și care se termină cu doi de 1 consecutivi, indicând faptul că următorul bit constituie începutul primului octet din adresa destinație ;
- AD - Adresa destinație - identifică stația ce trebuie să recepționeze cadrul.
- AS -Adresa sursă - adresa stației ce a emis cadrul ;
- TIP/LUNGIME- indică numărul de biți de date conținuți în câmpul de date al cadrului.
- DATE - o secvență de date de maxim 1500 de octeți. Dacă lungimea cadrului de date este inferioară valorii de 46 de octeți, este nevoie să se completeze restul biților până se ajunge la valoarea minimă impusă de standard (tehnică cunoscută sub numele de padding) ;
- CRC - semnalizează apariția unor eventuale erori în cadrul de transmisie.

<sup>1</sup> [www.ethermanage.com/ethernet/ethersname.html](http://www.ethermanage.com/ethernet/ethersname.html)

Cu toate progresele făcute, formatul cadrelor nu s-a schimbat, astfel încât toate rețelele Ethernet pot fi interconectate fără probleme

Fiecare calculator echipat Ethernet poartă denumirea de stație.

Arhitectura Ethernet este o arhitectură populară deoarece oferă echilibru între viteză, preț și instalare facilă.

### Arhitectura Token Ring

Este integrată în sistemele mainframe, dar și la conectarea calculatoarelor personale în rețea. Folosește o tehnologie fizică stea-cablată înel numită Token Ring. Astfel, văzută din exterior rețeaua pare a fi proiectată ca o stea, calculatoarele fiind conectate la un hub central, numit unitate de acces multiplu (MAU sau MSAU- Multi Station Access Unit), iar în interiorul echipamentului cablajul formează o cale de date circulară, creând un inel logic.

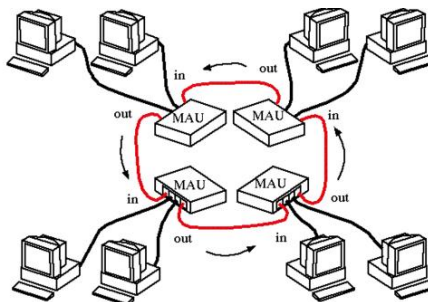


Fig.2.2. Arhitectura Token-Ring

Arhitectura folosește topologia logică de pasare a jetonului. Inelul logic este creat astfel de jetonul care se deplasează printr-un port al MSAU către un calculator. Dacă respectivul calculator nu are date de transmis, jetonul este trimis înapoi către MSAU și apoi pe următorul port către următorul calculator. Acest proces continuă pentru toate calculatoarele, dând astfel impresia unui inel fizic.

Folosește ca mediu de transmisie a datelor cablul torsadat, cablul coaxial sau fibra optică

**Arhitectura FDDI** (Fiber Distributed Data Interface), bazată pe topologia logică Token Ring, folosește fibra optică și funcționează pe o topologie fizică de tip inel dublu. Inelul dublu este alcătuit dintr-un inel principal, folosit pentru transmiterea datelor, și un inel secundar, folosit în general pentru back-up (linie de siguranță). Prin aceste inele, traficul se desfășoară în sensuri opuse. În mod normal, traficul folosește doar inelul principal. În cazul în care acesta se defectează, datele o să circule în mod automat pe inelul secundar în direcție opusă. Un inel dublu suportă maxim 500 de calculatoare pe inel. Lungimea totală a fiecărui inel este de 100 km și se impune amplasarea unui repetor care să regenereze semnalele la fiecare 2 km. Inelul principal oferă rate de transfer de până la 100 Mbps, iar dacă cel de-al doilea inel nu este folosit pentru backup, capacitatea de transmisie poate fi extinsă până la 200 Mbps.

În FDDI se întâlnesc două categorii de stații, fiecare având două porturi prin care se conectează la cele două inele:

- stații de clasă A, atașate ambelor inele
- stații de clasă B atașate unui singur inel

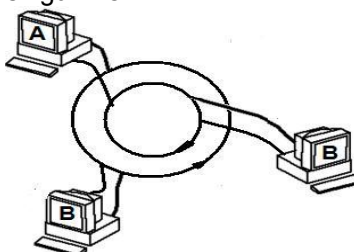


Fig.2.3. Rețea FDDI

### Tema 3 Standarde Ethernet

#### Fișa suport Standarde pentru rețele Ethernet

Acest material vizează competența / rezultat al învățării : **Analizează arhitectura și standardele rețelelor de date.**

Standardizarea asigură compatibilitatea echipamentelor care folosesc aceeași tehnologie. Există numeroase organizații de standardizare, care se ocupă cu crearea de standarde pentru rețelele de calculatoare.

IEEE (The Institute of Electrical and Electronic Engineers) este o asociație profesională tehnică nonprofit fondată în 1884, formată din peste 3777000 de membrii din 150 de țări, cu ocupații diferite – ingineri, oameni de știință, studenți. IEEE este foarte cunoscut pentru dezvoltarea standardelor pentru industria calculatoarelor și electronicelor în particular.

Pentru a asigura compatibilitatea echipamentelor într-o rețea Ethernet, IEEE a dezvoltat o serie de standarde recomandate producătorilor de echipamente Ethernet. Au fost elaborate astfel:

- Standarde pentru rețele cu cabluri
- Standarde pentru rețele cu fir

#### Standarde pentru rețele cu cabluri

În cazul rețelelor cu arhitectură Ethernet și mediu de transmisie a datelor prin cablu, a fost elaborat standardul IEEE 802.3

Au fost implementate o serie de tehnologii care respectă standardul Ethernet 802.3. dintre acestea cele mai comune sunt: 10BASE-T, 100 BASE-TX (cunoscută și sub numele de Fast Ethernet deoarece dezvoltă o lățime de bandă mai mare decât precedentă), 1000BASE-T (cunoscută și sub numele de Gigabit Ethernet), 10BASE-FL, 100BASE-FX, 1000BASE-SX, 1000BASE-LX

Numărul din partea stângă a simbolului ilustrează valoarea în Mbps a lățimii de bandă a aplicației

Termenul BASE ilustrează faptul că transmisia este baseband – întreaga lățime de bandă a cablului este folosită pentru un singur tip de semnal

Ultimele caractere se referă la tipul cablului utilizat ( T-indică un cablu torsadat, F ,L și S indică fibra optică)

Avantajele și dezavantajele tehnologiilor Ethernet dezvoltate în medii de transmisie prin cablu sunt ilustrate în tabela de mai jos:

Tehnologia	Avantaje	Dezavantaje
<b>10BASE-T</b>	Costuri de instalare mici în comparație cu fibra optică Sunt mai ușor de instalat decât cablurile coaxiale Echipamentul și cablurile sunt ușor de îmbunătățit	Lungimea maximă a unui segment de cablu este de doar 100 m Cablurile sunt susceptibile la interferențe electromagnetice
<b>100BASE-TX</b>	Costuri de instalare mici în comparație cu fibra optică Sunt mai ușor de instalat decât cablurile coaxiale Echipamentul și cablurile sunt ușor de îmbunătățit Lățimea de bandă este de 10 ori mai mare decât în cazul tehnologiilor 10BASE-T	Lungimea maximă a unui segment de cablu este de doar 100 m Cablurile sunt susceptibile la interferențe electromagnetice
<b>1000BASE-T</b>	Lățimea de bandă de până la 1 GB Suportă interoperabilitatea cu 10BASE-T și cu 100BASE-TX	Lungimea maximă a unui segment de cablu este de doar 100 m Cablurile sunt susceptibile la interferențe electromagnetice Cost ridicat pentru plăci de rețea și switch-uri Gigabit Ethernet Necesită echipament suplimentar

#### Standarde Ethernet pentru rețele fără fir

În cazul rețelelor cu arhitectură Ethernet și mediu de transmisie a datelor fără fir, IEEE a elaborat standardul IEEE 802.11 sau Wi-Fi. Acesta este compus dintr-un grup de standarde , pentru care sunt

specificate frecvența semnalelor de transmisie radio, lățimea de bandă , raza de acoperire și alte capabilități :

	Lățime bandă	Frecvență	Raza de acțiune	Interoperabilitate
<b>IEEE 802.11a</b>	Până la 54 Mbps	5 GHz	45,7 m	Incompatibil cu IEEE 802.11b, IEEE 802.11g, IEEE 802.11n
<b>IEEE 802.11b</b>	Până la 11 Mbps	2,4 GHz	91 m	Compatibil cu IEEE 802.11g
<b>IEEE 802.11g</b>	Până la 54 Mbps	2,4 GHz	91 m	Compatibil cu IEEE 802.11b
<b>IEEE 802.11n</b>	Până la 540 Mbps	2,4 GHz	250 m	Compatibil cu IEEE 802.11b și cu IEEE 802.11g

## Tema 4 Modele de date

### Fișa suport Modelul OSI și TCP/IP

Pentru a descrie modul de comunicare în rețea a două calculatoare, Andrew Tanenbaum l-a comparat cu discuția între doi filozofi care vorbesc limbi diferite, dar au aceleași raționament. Între ei se interpun câte un translator, și apoi câte o secretară.

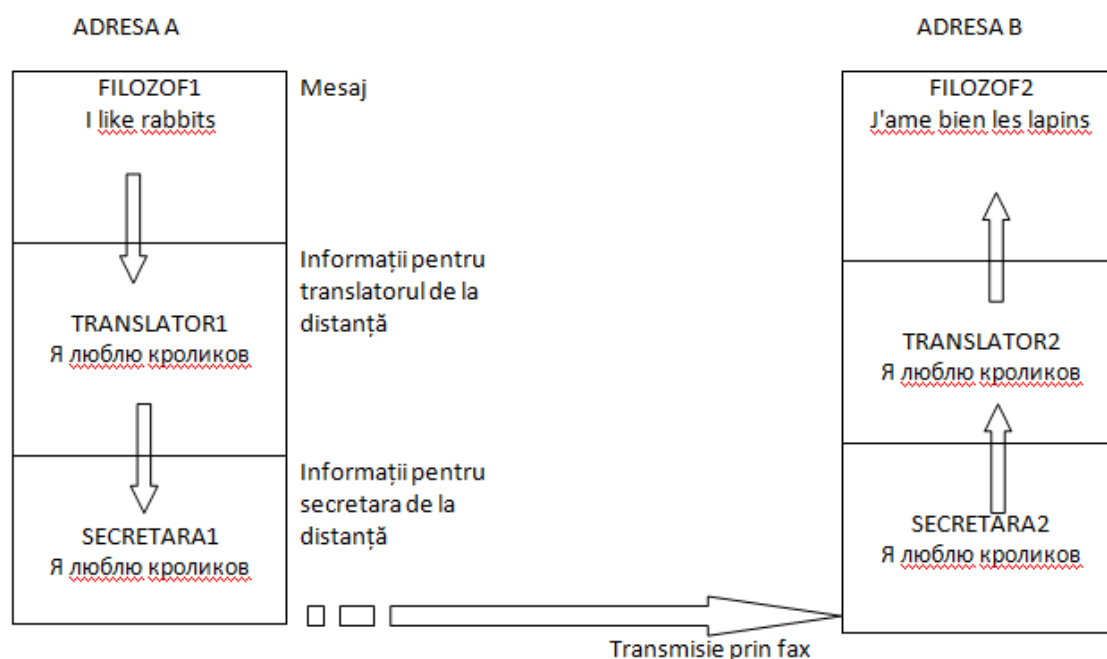


Fig.4.1. Comunicarea pe nivele

Pornind de la acest exemplu, putem aprecia că *nivelul n* al unui calculator nu poate comunica în mod direct cu *nivelul n* al altui calculator ci doar prin nivelul inferior. Prin urmare, se presupune că regulile folosite în comunicare se numesc *protocoale de nivel n*.

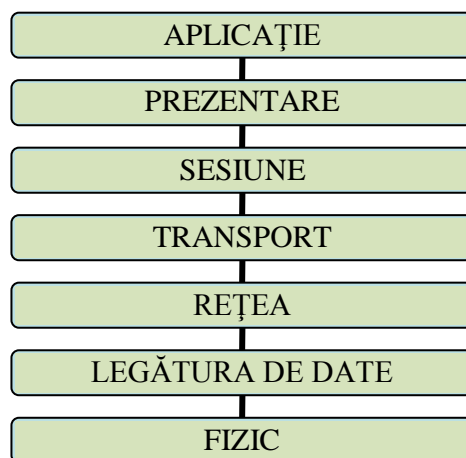


Conceptul de model de date a fost implementat cu scopul de a separa funcțiile protocoalelor de comunicație pe niveluri ușor de administrat și de înțeles, astfel încât fiecare nivel să realizeze o funcție specifică în procesul de comunicare în rețea. Conceptul de nivel este folosit pentru a descrie acțiunile și procesele ce apar în timpul transmiterii informațiilor de la un calculator la altul.

Într-o rețea, comunicarea are loc prin transferul de informații de la un calculator-sursă spre un calculator-destinație. Informațiile care traversează rețeaua sunt referite ca date, pachete sau pachete de date.

## Modelul OSI (Open Systems Interconnect)

A fost creat de Organizația Internațională de Standardizare (International Standards Organization - ISO) cu scopul de a standardiza modul în care echipamentele comunică în rețea, și a fost definit în standardul ISO 7498-1. Modelul OSI are 7 niveluri și este cel mai frecvent utilizat de producătorii de echipamente de rețea.



În modelul OSI, la transferul datelor, se consideră că acestea traversează virtual de sus în jos nivelurile modelului OSI al calculatorului sursă și de jos în sus nivelurile modelului OSI al calculatorului destinație.



Nivelul **Aplicație** asigură interfața cu aplicațiile utilizator și transferul informațional între programe. La acest nivel se definește accesul aplicațiilor la serviciile de rețea și implicit comunicația între două sau mai multe aplicații.



Nivelul **Prezentare** se ocupă de sintaxa și semantica informațiilor transmise între aplicații sau utilizatori. La acest nivel se realizează conversia datelor din formatul abstract al aplicațiilor în format acceptat de rețea, compresia și criptarea datelor pentru a reduce numărului de biți ce urmează a fi transmiși, redirectionarea datelor pe baza de cereri.



Nivelul **Sesiune** asigură stabilirea, gestionarea și închiderea sesiunilor de comunicație între utilizatorii de pe două stații diferite. Prin sesiune se înțelege dialogul între două sau mai multe entități. Nivelul sesiune sincronizează dialogul între nivelurile sesiune ale entităților și gestionează schimbul de date între acestea. În plus, acest nivel oferă garanții în ceea ce privește expedierea datelor, clase de servicii și raportarea erorilor. În câteva cuvinte, acest nivel poate fi asemuit cu dialogul uman.



Nivelul **Transport** este nivelul la care are loc segmentarea și reasamblarea datelor. El furnizează un serviciu pentru transportul datelor către nivelurile superioare, și în special caută să vadă cât de sigur este transportul prin rețea. Nivelul transport oferă mecanisme prin care stabilește, întreține și ordonă închiderea circuitelor virtuale; detectează "căderea" unui transport și dispune refacerea acestuia; controlează fluxul de date pentru a preveni rescrierea acestora. Sarcina principală a nivelului transport este aceea de refacere a fluxului de date la destinație, deoarece datele sunt fragmentate în segmente mai mici, cu rute diferite prin rețeaua de comunicații.


În cazul utilizării protocolului IP pe nivelul rețea, sunt disponibile două protocoale la nivelul transport:

- TCP, Transmission Control Protocol este un protocol bazat pe conexiune, în care pentru fiecare pachet transmis se așteaptă o confirmare din partea echipamentului de destinație. Transmiterea următorului pachet nu se realizează dacă nu se primește confirmarea pentru pachetul transmis anterior.

- UDP, User Datagram Protocol este folosit în situațiile în care eficiența și viteza transmisiei sunt mai importante decât corectitudinea datelor, de exemplu în rețelele multimedia, unde pentru transmiterea către clienți a informațiilor de voce sau imagine este mai importantă viteza (pentru a reduce întreruperile în transmisie) decât calitatea. Este un protocol fără conexiuni, semnalarea erorilor fiind asigurată de nivelul superior, iar datele transmise nu sunt segmentate.




Nivelul **Rețea** Este unul dintre cele mai complexe niveluri; asigură conectivitatea și selecția căilor de comunicație între două sisteme ce pot fi localizate în zone geografice diferite. La acest nivel, se evaluează adresele sursă și destinație și se fac translațiile necesare între adrese logice (IP) și fizice (MAC). Funcția principală a acestui nivel constă în dirijarea pachetelor între oricare două noduri de rețea. Cu alte cuvinte, nivelul rețea realizează „rutarea” (direcționarea) pachetelor de date prin infrastructura de comunicații, această operație fiind efectuată la nivelul fiecărui nod de comunicație intermediar. Nivelul rețea asigură interfața între furnizorul de servicii și utilizator, serviciile oferite fiind independente de tehnologia subrețelei de comunicație.

 Nivelul **Legăturii de date** gestionează transmisia biților de date, organizați în cadre, fără erori nedetectate, relativ la o anumită linie de transmisie. Schimbul de cadre între sursă și destinatar presupune trimiterea secvențială a acestora urmată de cadre de confirmare a recepției. Principalele atribuții ale acestui nivel au în vedere controlul erorilor, controlul fluxului informațional și gestiunea legăturii.

Acest nivel este format din două subnivele:

- MAC (Medium Access Control) – control al accesului la mediu
- LLC (Logical Link Control) – legatura logica de date

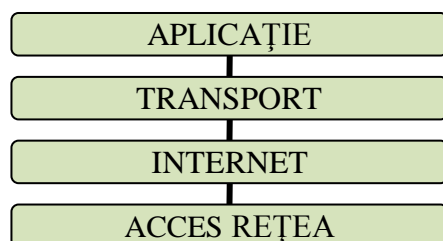
 Nivelul **Fizic**, este nivelul la care biții sunt transformați în semnale (electrice, optice) Standardele asociate nivelului fizic conțin specificații electrice (parametrii de semnal, proprietăți ale mediului de comunicație) și mecanice (conectică, cabluri). Ca atribuții nivelul fizic se ocupă de codarea și sincronizarea la nivel de bit, delimitând lungimea unui bit și asociind acestuia impulsul electric sau optic corespunzător canalului de comunicație utilizat. La acest nivel se definesc:


- tipul de transmitere și recepționare a șirurilor de biți pe un canal de comunicații
- topologiile de rețea
- tipurile de medii de transmisiune : cablu coaxial, cablu UTP, fibră optică, linii închiriate de cupru etc.
- modul de transmisie: simplex, half-duplex, full-duplex
- standardele mecanice și electrice ale interfețelor
- este realizată codificarea și decodificarea șirurilor de biți
- este realizată modularea și demodularea semnalelor purtătoare (modem-uri).


Modelul OSI	Nivelul	Descriere
Aplicație	7	Asigură interfața cu utilizatorul
Prezentare	6	Codifică și convertește datele
Sesiune	5	Construiește, gestionează și închide o conexiune între o aplicație locală și una la distanță
Transport	4	Asigură transportul sigur și menține fluxul de date dintr-o rețea
Rețea	3	Asigură adresarea logică și domeniul de rutare
Legătură de date	2	Pachetele de date sunt transformate în octeți și octeții în cadre. Asigură adresarea fizică și procedurile de acces la mediu
Fizic	1	Mută șiruri de biți între echipamente Definește specificațiile electrice și fizice ale echipamentelor

### Modelul TCP/IP (Transport Control Protocol/Internet Protocol)

Modelul de referință TCP/IP a fost creat de cercetătorii din U.S.Department of Defense (DoD), este folosit pentru a explica suita de protocoale TCP/IP, și are 4 niveluri:



 Protocoalele de nivel *Aplicație* oferă servicii de rețea aplicațiilor utilizator cum ar fi browserele web și programele de e-mail. Câteva exemple de protocoale definite la acest nivel sunt TELNET, FTP, SMTP, DNS, HTTP

 Protocoalele la nivel *Transport* oferă administrarea de la un capăt la altul a transmisiei de date. Una din funcțiile acestor protocoale este de a împărți datele în segmente mai mici pentru a fi transportate ușor peste rețea. La nivelul Transport funcționează protocoalele TCP(Transmission Control Protocol) și UDP(User Datagram Protocol) Acest nivel oferă servicii de transport între sursă și destinație, stabilind o conexiune logică între sistemul emițător și sistemul receptor din rețea





Protocoloalele la nivel *Internet* operează la nivelul trei (începând de sus) al modelului TCP/IP. Aceste protocoale sunt folosite pentru a oferi conectivitate între stațiile din rețea. La nivelul *Internet* funcționează protocolul IP (Internet Protocol) Nivelul *Internet* are rolul de a permite sistemelor gazdă să trimită pachete în orice rețea și să asigure circulația independentă a pachetelor până la destinație. Pachetele de date pot sosi într-o ordine diferită de aceea în care au fost transmise, rearanjarea lor în ordine fiind sarcina nivelurilor superioare



Protocoloalele de nivel *Acces rețea* descriu standardele pe care stațiile le folosesc pentru a accesa mediul fizic. Standardele și tehnologiile Ethernet IEEE 802.3, precum și CSMA/CD și 10BASE-T sunt definite pe acest nivel. Nivelul *Acces rețea* – se ocupă de toate conexiunile fizice pe care trebuie să le străbată pachetele IP pentru a ajunge în bune condiții la destinație.

Cele patru niveluri realizează funcțiile necesare pentru a pregăti datele înainte de a fi transmise pe rețea. Un mesaj pornește de la nivelul superior (nivelul Aplicație) și traversează de sus în jos cele patru niveluri până la nivelul inferior (nivelul Acces rețea). Informațiile din header sunt adăugate la mesaj în timp ce acesta parcurge fiecare nivel, apoi mesajul este transmis. După ce ajunge la destinație, mesajul traversează din nou, de data aceasta de jos în sus fiecare nivel al modelului TCP/IP. Informațiile din header care au fost adăugate mesajului sunt înlăturate în timp ce acesta traversează nivelurile destinație.

Modelul TCP/IP	Stratul	Descriere
Aplicație	4	La acest nivel funcționează protocoalele la nivel înalt (SMTP și FTP)
Transport	3	La acest nivel are loc controlul de debit/flux și funcționează protocoalele de conexiune
Internet	2	La acest nivel are loc adresarea IP
Acces rețea	1	La acest nivel are loc adresarea după MAC și componentele fizice ale rețelei

Dacă am compara modelul OSI cu modelul TCP/IP, am observa că între ele există o serie de asemănări dar și deosebiri.

Ambele modele de date descriu procesul de comunicație a datelor în rețea pe nivele și ambele conțin nivelele Aplicație și Transport, cu funcții asemănătoare. Spre deosebire de modelul OSI care folosește șapte niveluri, modelul TCP/IP folosește patru. Astfel, nivelurile OSI sesiune și prezentare sunt tratate de de nivelul TCP/IP aplicație, respectiv, nivelurile OSI legătură de date și fizic de nivelul acces rețea. Modelul OSI este folosit pentru dezvoltarea standardelor de comunicație pentru echipamente și aplicații ale diferiților producători, pe când modelul TCP/IP este folosit pentru suita de protocoale TCP/IP.

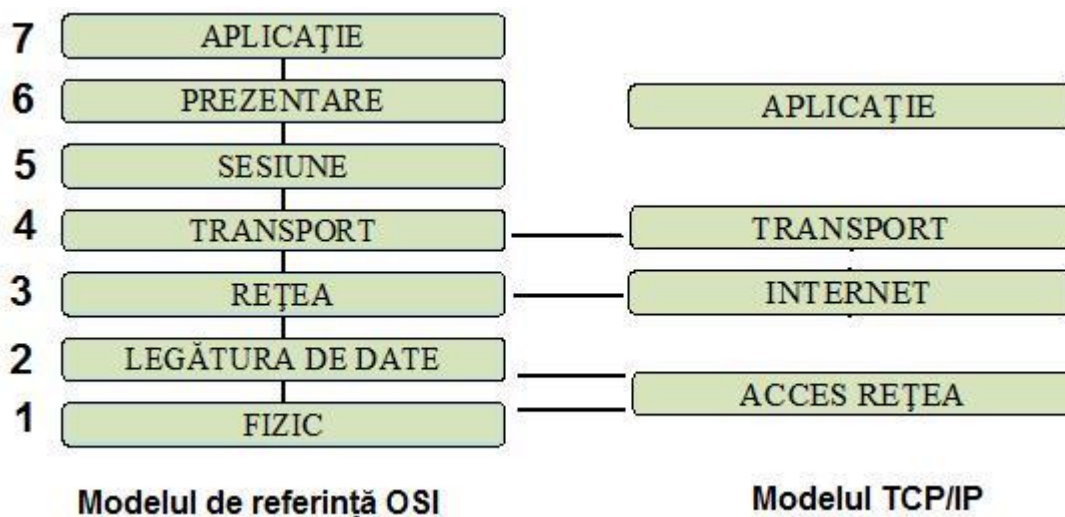


Fig 4.2. Modelele de date OSI și TCP/IP



## Tema 5 Adresarea IP

### Fisa suport 5.1 Structura unei adrese IP



O adresă este un număr sau o înșiruire de caractere care identifică în mod unic un echipament conectat într-o rețea, servind la comunicarea cu celelalte echipamente ale rețelei.

Cu ajutorul adresei, un calculator poate fi localizat într-o rețea de către altul. Un calculator poate fi conectat simultan la mai multe rețele. În acest caz, acesta va avea asociate mai multe adrese, fiecare adresă îl va localiza în una din rețelele la care este conectat.



**Adresa fizică** - cum este adresa MAC (Media Access Control) atribuită plăcii de rețea - este o adresă care este fixă, nu poate fi schimbată - cum este pentru o persoană, de exemplu, codul numeric personal



**Adresa logică** - Adresa IP (Internet Protocol), sau adresa de rețea - este atribuită fiecărei stații de către administratorul de rețea și poate fi regenerată - cum ar fi pentru o persoană, de exemplu, adresa la care locuiește.

### Adresarea IPv4



Adresa IPv4 este o versiune pe 32 de biți a adresei IP. Este formată din 32 de cifre binare (1 și 0), grupate în patru bucăți de câte 8 biți, numiți octeți. Pentru a putea fi citită de către oameni, fiecare octet este reprezentat prin valoarea sa zecimală, separat de ceilalți octeți prin câte un punct. Altfel spus, adresa IPv4 este formată din patru numere zecimale cuprinse între 0 și 255 și separate prin puncte.

De exemplu, reprezentarea în binar: "01111101 00001101 01001001 00001111" corespunde reprezentării zecimale: "125.13.73.15."

O adresă IP este un tip de adresare ierarhică și din acest motiv este compusă din două părți. Prima parte - Rețea - identifică rețeaua căreia îi aparține un echipament și a doua parte - Gazdă - identifică în mod unic dispozitivul conectat la rețea.

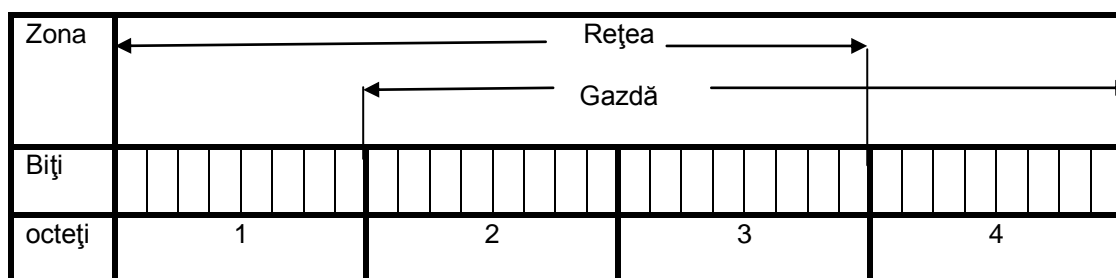


Fig 5.1. Structura unei adrese IP pe 32 de biți

Astfel, orice adresă IP identifică un echipament din rețea și rețeaua căreia îi aparține.

Într-o rețea, gazdele pot comunica între ele doar dacă au același identificador de rețea. Dacă au identificatori de rețea diferiți comunicarea se face prin intermediul unor dispozitive specializate în conexiuni.



Adresele IP care au toți biții identicatorului gazdă egali cu 0 sunt rezervate pentru adrese de rețea.



Adresele IP care au toți biții identicatorului gazdă egali cu 1 sunt rezervate pentru adrese de broadcast. Adresa de broadcast permite unei stații din rețea să transmită date simultan către toate echipamentele din rețea (să difuzeze)

Teoretic, adresarea IPv4 acoperă adrese (în baza 10) între 0.0.0.0 și 255.255.255.255,

în total în număr de  $2^{32}$

### Adresarea IPv6

La sfârșitul anilor 90' s-a răspândit vestea că adresele IP în clasă B vor fi epuizate, fapt ce ar fi condus la compromiterea sistemului de adresare pe Internet, singura soluție viabilă pe termen lung fiind reprezentată de crearea unui nou IP cu adresare pe 128 de biți (IPv6-Internet Protocol versiunea 6 sau IPng - Internet Protocol New Generation). Versiunea 6 de IP mărește numărul de adrese viabile la  $2^{128}$ .

## Fisa suport 5.2. Clase de adrese IP

Pentru a gestiona eficient adresele IP acestea au fost împărțite în clase care diferă prin numărul de biți alocați pentru identificarea rețelei respectiv numărul de biți alocați pentru identificarea unui dispozitiv (gazda, stația, host) în cadrul unei rețele. Există cinci clase de adrese IP: A, B, C, D și E.

- Clasa A – primul bit are valoarea 0, primul octet este alocat pentru identificarea rețelei, următorii trei octeți sunt alocați pentru identificarea gazdei - pentru rețele mari, folosite de companii mari și de unele țări.

REȚEA	GAZDĂ	GAZDĂ	GAZDĂ
-------	-------	-------	-------

- Clasa B - primii doi biți au valoarea 10, primii doi octeți sunt alocați pentru identificarea rețelei, următorii doi octeți sunt alocați pentru identificarea gazdei - pentru rețele de dimensiuni medii, cum ar fi cele folosite în universități

REȚEA	REȚEA	GAZDĂ	GAZDĂ
-------	-------	-------	-------

- Clasa C - primii trei biți au valoarea 110, primii trei octeți sunt alocați pentru identificarea rețelei, ultimul octet este alocat pentru identificarea gazdei - pentru rețele de dimensiuni mici, atribuite de furnizorii de servicii de Internet clienților lor

REȚEA	REȚEA	REȚEA	GAZDĂ
-------	-------	-------	-------

- Clasa D – primii patru biți au valoarea 1110, toți cei patru octeți sunt alocați pentru identificarea rețelei - folosită pentru multicast

REȚEA	REȚEA	REȚEA	REȚEA
-------	-------	-------	-------

- Clasa E – folosită pentru testare

CLASA	Începe cu...	Identificator rețea	Identificator gazdă	Nr. rețele	Nr. gazde	Intervalul de adrese
A	0	primul octet	ultimii trei octeți	127	16.777.214	1.0.0.0 – 126.0.0.0
B	10	primii doi octeți	ultimii doi octeți	16.382	65.543	128.1.0.0 – 191.254.0.0
C	110	primii trei octeți	ultimul octet	2.097.150	254	192.0.1.0 – 223.255.254.0

### Adrese private

IANA (Internet Assigned Numbers Authority) a definit ca spațiu de adresare privată intervalele: 10.0.0.0 - 10.255.255.255 (clasa A), 172.16.0.0 - 172.31.255.255 (clasa B), 192.168.0.0 - 192.168.255.255 (clasa C). Totodată intervalul 169.254.0.0 - 169.254.255.255 este rezervat pentru adresarea IP automată privată (APIPA - Automatic Private IP Addressing) utilizată pentru alocarea automată a unei adrese IP la instalarea inițială a protocolului TCP/IP peste anumite sisteme de operare. Adresele private sunt ignorate de către echipamentele de rutare, ele putând fi utilizate pentru conexiuni nerutate, în rețelele locale. Pentru clasele A, adresa de rețea 127.0.0.1 este de asemenea rezervată pentru teste în bucla închisă. Restul adreselor au statutul de adrese IP publice beneficiind de vizibilitate potențială la nivelul rețelei mondiale Internet.

## Fisa suport 5.3 Adresarea IP în subrețele

De multe ori, în practică, administratorii de rețea sunt nevoiți să împartă o rețea în mai multe rețele LAN de dimensiuni mai mici (subrețele). Împărțirea logică a unei rețele în subrețele se întâlnește sub numele de subnetare.



Deoarece gazdele dintr-o subrețea „se văd” numai între ele înseamnă că trebuie să se definească punctul de ieșire/intrare în rețea, adică o adresă IP din interiorul subrețelei respective asociată dispozitivului de rutare (interconectarea cu alte subrețele). Acest punct comun sistemelor din subrețea se numește poarta de acces (gateway).

Adresele pentru subrețele sunt unice, au 32 de biți, și conțin trei identificatori

Rețea	Subrețea	Gazdă
-------	----------	-------

**Rețea:** numărul de indentificare a rețelei

**Subrețea:** numărul de indentificare a subrețelei

**Gazdă:** numărul de indentificare a gazdei.

Pentru a crea o subrețea, administratorul va împrumuta un număr de minim 2 biți din secțiunea gazdă a unei clase și să îi folosească în cadrul câmpului subrețea. Dacă s-ar împrumuta un singur bit, am ajunge în situația de a avea doar o adresă de rețea (pt val 0 a bitului împrumutat) și o adresă de broadcast(pentru val 1). Din același motiv, în zona gazdă trebuie să rămână minim 2 biți.

Pentru a asigura inter-vizibilitatea dispozitivelor dintr-o subrețea s-a introdus noțiunea de mască de (sub)rețea.



Termenul de *mască de subrețea* (subnet mask), sau prefix, se referă la un identificator care este tot un număr pe 32 de biți, ca și adresa IP, și care are rolul de a indica partea dintr-o adresă IP care este identificatorul rețelei, partea care este identificatorul subrețelei și partea care este identificatorul stației. La măștile de subrețea, biții din porțiunea rețea și subrețea au valoarea 1, iar cei din porțiunea stație, au valoarea 0. Biții folosiți pentru a defini rețeaua și subrețeaua formează împreună prefixul extins de rețea.

Măștile de rețea implicite pentru clasele A, B și C sunt ilustrate în tabelul de mai jos:

Clasa	Masca de rețea implicită	Număr de gazde
A	255.0.0.0	$2^{24}-2$
B	255.255.0.0	$2^{16}-2$
C	255.255.255.0	$2^8-2$

Să luăm ca exemplu o adresă 193.234.57.34, care este o adresă IP de clasă C cu masca de subrețea 255.255.255.224. Valoarea 224 a ultimului octet a măștii, care este diferită de 0 ne sugerează faptul că stația face parte dintr-o subrețea.

Masca de subretea	Baza 10	255	255	255	224
	Baza 2	11111111	11111111	11111111	11100000

Cum ultimul octet din masca de subrețea are valoarea 224(10)= 11100000(2), primii trei biți au valoarea 1, ceea ce înseamnă că porțiunea rețea a fost extinsă cu 3 biți, ajungând la un total de 27, în timp ce numărul biților atribuiți gazdelor, și care au valoarea 0, a fost redus la 5.



Numărul de subrețele posibile matematic depinde de tipul clasei din care face parte segmentul de adrese IP care este subnetat. De fiecare dată când se împrumută câte 1 bit din porțiunea gazdă a unei adrese, numărul subrețelilor create crește cu 2 la puterea numărului de biți împrumutați. Prima și ultima subrețea fac parte din categoria celor rezervate, fiind deci inutilizabile. De fiecare dată când se împrumută 1 bit din porțiunea gazdă a unei adrese, numărul adreselor disponibile pentru o subrețea se reduce cu o putere a lui 2. În cazul subrețelilor, prima adresa (numele subrețelei, toți biții măștii cu valoarea „1”) și ultima (adresa de trimitere multiplă, broadcast, toți biții măștii pe „0”) nu sunt folosibile pentru adresarea gazdelor, deci la fiecare subrețea „se pierde” două adrese. La o subrețea de 4 adrese 2 nu sunt exploatabile iar o subrețea de 2 adrese nu are sens.

De exemplu, pentru adresele din clasa C, cu masca de rețea 255.255.255.224, se pot obține 8 subrețele (23) din care doar 6 sunt utilizabile, numărul maxim al gazdelor pentru fiecare subrețea este de 32(25) din care doar 30 sunt utilizabile.

În tabelul de mai jos este exemplificată împărțirea în subrețele a rețelelor de clasă C

Număr de biți împrumutați identificatorului de rețea	Masca de subrețea	Număr de adrese de subrețea utilizabile	Număr de adrese- gazdă pe subrețea
2	255.255.255.192	2	62
3	255.255.255.224	6	30
4	255.255.255.240	14	14
5	255.255.255.248	30	6
6	255.255.255.252	62	2



Adresa subrețelei din care face parte o stație se calculează înmulțind logic în binar (aplicând operatorul logic AND) adresa IP a stației cu masca de subrețea. Porțiunea gazdă a adresei se pierde pentru că devine 0

De exemplu, pentru stația cu adresa IP 192.168.100.40, cu masca de rețea 255.255.255.224 se poate calcula adresa subrețelei din care face parte astfel:

Adresa IP gazdă 192.168.100.40	11000000	10101000	01100100	00101000
	AND			
Masca de subrețea 255.255.255.224	11111111	11111111	11111111	11100000
	=			
Subrețea 192.168.100.32	11000011	10101000	01100100	00100000

Prin urmare, stația exemplificată face parte din subrețeaua 192.168.100.32

Subnetarea într-un număr dat de subrețele

De exemplu, se cere să subnetăm rețeaua 192.168.100.0 (care este o rețea de clasă C) în 8 subrețele .

Masca de rețea implicită este

255.255.255.0 (11111111.11111111.11111111.00000000)

Va trebui să sacrificăm 3 biți din secțiunea gazdă, pentru a forma profilul extins de rețea. Ultimul octet al măștii de subrețea va avea valoarea în binar 11100000 adică valoarea 224 în zecimal. Prin urmare, masca de subrețea va fi

255.255.255.224 (11111111.11111111.11111111.11100000)

Din 256 (echivalentul lui 28) scădem valoarea zecimală a ultimului octet din masca de subrețea:

256-224=32

Adresele de subrețea vor fi multiplu de 32

Subrețea	Adresa IP a subrețelei	Adresele gazdelor	Adresa de broadcast
Baza	192.168.100.0		
Subrețea 0	192.168.100.0	Rezervat	Nici una
Subrețea 1	192.168.100.32	.33 la .62	192.168.100.63
Subrețea 2	192.168.100.64	.65 la .94	192.168.100.95
Subrețea 3	192.168.100.96	.97 la .126	192.168.100.127
Subrețea 4	192.168.100.128	.129 la .158	192.168.100.159
Subrețea 5	192.168.100.160	.161 la .190	192.168.100.191
Subrețea 6	192.168.100.192	.193 la .222	192.168.100.223
Subrețea 7	192.168.100.224	Rezervat	Nici una

Subrețele 0 și 7, nu sunt în mod normal utilizabile, ele făcând parte din categoria celor rezervate. Adresele IP ale subrețelilor sunt definite incrementând valoarea zecimală a ultimului octet cu 32. Adresele gazdelor din fiecare subrețea se obțin incrementând valoarea zecimală a ultimului octet cu 1. Sunt posibile 32 de adrese, prima și ultima fiind însă rezervate așa cum s-a arătat anterior. Rezultă un număr utilizabil de 30 de gazde pentru fiecare subrețea.

Un dispozitiv cu adresa IP 192.168.100.33 ar fi prima gazdă din subrețeaua 1. Următoarele gazde ar fi numerotate până la 192.168.100.62, moment în care subrețeaua ar fi complet populată și nu ar mai putea fi adăugate noi gazde

## Tema 6 Serviciul de rezolvare a numelui

### Fișa suport Descrierea serviciului DNS

DNS (Domain Name System) – este un serviciu care permite referirea calculatoarelor gazdă cu ajutorul adresei literale.

Adresa literală conține succesiuni de nume asociate cu domenii, subdomenii sau tipuri de servicii. Acest mod de adresare este utilizat exclusiv de nivelul aplicație și este util deoarece permite operatorului uman să utilizeze o manieră prietenoasă și comodă de localizare a informațiilor. Forma generală a unei astfel de adrese este

[tip\_serviciu].[nume\_gazda].[subdomeniu2].[subdomeniu1].[domeniu].[tip\_domeniu]

Exemple: [www.edu.ro](http://www.edu.ro), <http://cisco.netacad.net> etc

Practic, serviciul DNS transformă adresa IP într-o adresă literală, și invers. Privit în amănunt, DNS este un soft care gestionează și controlează o bază de date distribuită, constituită dintr-o sumă de fișiere memorate pe calculatoare diferite-localizate în spații geografice diferite, ca pe o singură bază de date.

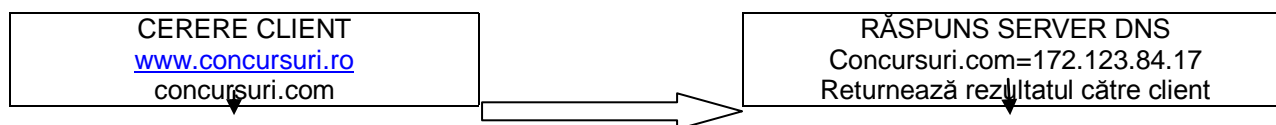


Fig 6.1. Formularea unei cereri către un server DNS

Conform figurii de mai sus, clientul dorește să acceseze de pe calculatorul său personal pagina web [www.concursuri.ro](http://www.concursuri.ro), această cerere este trimisă unui server DNS care o analizează și returnează ca rezultat adresa IP a stației care găzduiește site-ul solicitat.

În principiu, DNS este alcătuit din trei componente:

- *Spațiul numelor de domenii* – reprezintă informația conținută în baza de date, structurată ierarhic.
- *Servere de nume* – programe server care stochează informația DNS și răspund cererilor adresate de alte programe
- *Resolvele* – programe care extrag informațiile din serverele de nume ca răspuns la cererile unor clienți

Pentru a stabili corespondența dintre un nume și o adresă IP, programul de aplicație apelează un resolver, transferându-l numele ca parametru, resolverul trimite un pachet UDP (printr-un protocol de transport fără conexiune) la serverul DNS local, care caută numele și returnează adresa IP către resolver, care o trimite mai departe apelantului. Înmarmat cu adresa IP, programul poate stabili o conexiune TCP cu destinația sau îi poate trimite pachete UDP.

În continuare ne vom referi mai în amănunt la spațiul numelor de domenii.

Internetul este divizat în peste 200 de domenii de nivel superior, fiecare domeniu superior este divizat la rândul său în subdomenii, acestea la rândul lor în alte subdomenii, etc. Domeniile de pe primul nivel se împart în două categorii :generice (com, edu, gov, int, mil, net, org) și de țări (cuprind câte o intrare pentru fiecare țară, de exemplu pentru România : ro).

Fiecărui domeniu, fie că este un calculator-gazdă, fie un domeniu superior, îi poate fi asociată o mulțime de înregistrări de resurse (resource records). Deși înregistrările de resurse sunt codificate binar, în majoritatea cazurilor ele sunt prezentate ca text, câte o înregistrare de resursă pe linie. Un exemplu de format este:

#### Nume\_domeniu Timp\_de\_viață Clasă Tip Valoare

- *Nume\_domeniu* precizează domeniul căruia i se aplică înregistrarea. În mod normal există mai multe înregistrări pentru fiecare domeniu
- *Timp\_de\_viață* exprimă, în secunde, cât de stabilă este înregistrarea. De exemplu, un timp de 60 de secunde este considerat a fi scurt, iar informația instabilă, pe când o valoare de ordinul a 80000 de secunde este o valoare mare, informația este considerată stabilă.
- *Tip* precizează tipurile înregistrării. Cele mai importante tipuri sunt prezentate mai jos:

Tip	Semnificație
A	Adresa IP a unui sistem gazdă
MX	Schimb de poștă
NS	Server de nume
CNAME	Nume canonic
PTR	Pointer

Înregistrarea A păstrează adresa IP a calculatorului gazdă

*MX* precizează numele calculatorului gazdă pregătit să accepte poșta electronică pentru domeniul specificat. Dacă cineva dorește de exemplu să trimită un mail lui paul@edu.ro, calculatorul care trimite

trebuie să găsească un server la edu.ro dispus să accepte mail. Această informație poate fi furnizată de înregistrarea MX

NS specifică serverele de nume. De exemplu fiecare bază de date DNS are în mod normal o înregistrare NS pentru fiecare domeniu de pe primul nivel.

Înregistrările CNAME permit crearea pseudonimelor. De exemplu, o persoană familiarizată cu atribuirea numelor în Internet, care dorește să trimită un mesaj unei persoane al cărui nume de conectare la un sistem de calcul din departamentul de calculatoare din cadrul Ministerului Educației este paul, poate presupune că adresa paul@dc.edu este corectă. De fapt, această adresă nu este corectă, domeniul departamentului de calculatoare de la Ministerul Educației fiind depc.edu. Ca un serviciu pentru cei care nu știu acest lucru, totuși, se poate genera o intrare CNAME pentru a dirija persoanele și programele în direcția corectă.

Tipul PTR se referă, la fel ca și CNAME la alt nume. Spre deosebire de CNAME care este în realitate o macro-definiție, PTR este un tip de date, utilizată în practică pentru asocierea unui nume cu o adresă IP, pentru a permite căutarea adresei IP și obținerea numelui sistemului de calcul corespunzător. Acest tip de căutare se numesc căutări inverse (reverse lookups).

- Valoare poate fi un număr, un nume de domeniu sau un cod ASCII

Exemplul de mai jos poate fi un mic segment dintr-o posibilă bază de date DNS pentru an.ofd.nl

an.ofd.nl	86400	A	194.43.54.234
ros.an.ofd.nl	86400	MX	2 iris.an.ofd.nl
www.an.ofd.nl	86400	CNAME	dream.an.ofd.nl

## Tema 7 Suita de protocoale TCP/IP

### Fișa suport Protocoale TCP/IP

Acest material vizează competența / rezultat al învățării : **Analizează protocolul TCP/IP.**



Un protocol de rețea reprezintă un set de reguli care guvernează comunicațiile între echipamentele conectate într-o rețea. Specificațiile protocoalelor definesc formatul mesajelor care sunt transmise și care sunt primite asigurând totodată și sincronizarea. Sincronizarea asigură un anumit interval de timp maxim pentru livrarea mesajelor, astfel încât calculatoarele să nu aștepte nedefinit sosirea unor mesaje care este posibil să se fi pierdut.

Protocoalele TCP/IP (Transport Control Protocol/Internet Protocol) sunt organizate pe nivelurile modelului de date TCP/IP și sunt caracterizate prin următoarele:

- Nu sunt specifice furnizorilor de echipamente;
- Au fost implementate pe orice tip de calculatoare începând cu calculatoare personale, minicalculatoare, calculatoare și supercalculatoare.
- Aceste protocoale sunt utilizate de către diverse agenții guvernamentale și comerciale din diverse oraș

**HTTP (Hyper Text transfer Protocol)** - Protocol de transfer al hypertextului –guvernează cum, de exemplu, fișierele de tip text, grafică, sunet și video sunt interschimbate pe Internet sau World Wide Web (www). Prin hypertext se înțelege o colecție de documente unite între ele prin legături (link) ce permit parcurgerea acestora bidirecțional.

Aplicațiile care folosesc acest protocol trebuie să poată formula cereri și/sau recepționa răspunsuri (modelul client-server). Clientul cere accesul la o resursă, iar serverul răspunde printr-o linie de stare (care conține, printre altele, un cod de succes sau eroare și, în primul caz, datele cerute).

Resursa trebuie să poată fi referită corect și fără echivoc. Pentru referirea unei resurse în Internet, se folosește termenul generic URI - Uniform Resource Identifier. Dacă se face referire la o locație spunem că avem de a face cu un URL - Universal Resource Locator. Dacă se face referire la un nume avem de-a face cu un URN- Universal Resource Name

Adresarea unei resurse în Internet se face prin construcții de forma:

protocol://[serviciu].nume\_dns[nume\_local/cale/subcale/nume\_document]

Cererile sunt transmise de software-ul client HTTP, care este și o altă denumire pentru un browser web.

Altfel spus, protocolul HTTP este specializat în transferul unei pagini web între browserul clientului și serverul web care găzduiește pagina respectivă. HTTP definește exact formatul cererii pe care browserul o trimite, precum și formatul răspunsului pe care serverul i-l returnează. Conținutul paginii este organizat cu ajutorul codului HTML (Hyper Text Markup Language), dar regulile de transport al acesteia sunt stabilite de protocolul http.

**TELNET** –este o aplicație destinată accesului, controlului și depanării de la distanță a calculatoarelor și a dispozitivelor de rețea. Acest protocol permite utilizatorului să se conecteze la un sistem de la distanță și să comunice cu acesta printr-o interfață. Folosind telnetul, comenzile pot fi date de pe un terminal amplasat la distanțe foarte mari față de computerul controlat, ca și când utilizatorul ar fi conectat direct la acesta. TelNet asigură o conexiune logică între cele două echipamente: cel controlat și cel folosit ca terminal numită sesiune telnet.



**FTP(File Transfer Protocol)** – este protocolul care oferă facilități pentru transferul fișierelor pe sau de pe un calculator din rețea. De multe ori pentru această acțiune utilizatorul este nevoit să se autentifice pe calculatorul de pe care dorește să încarce/descarce fișiere. Facilitatea cunoscută sub numele de anonymous ftp lucrează cu un cont public implementat pe calculatorul gazdă, numit guest.

În general, când se inițiază un transfer prin ftp trebuie precizate următoarele aspecte:

*Tipul fișierului.* - Se specifică maniera în care datele conținute de un fișier vor fi aduse într-un format transportabil prin rețea:

- fișiere ASCII – calculatorul care transmite fișierul îl convertește din formatul local text în format ASCII.
- fișiere EBCDIC – similar cu ASCII
- fișiere binare (binary) – fișierul este transmis exact cum este memorat pe calculatorul sursă și memorat la fel pe calculatorul destinație
- fișiere locale – folosite în mediile în care cel care transmite precizează numărul de biti/byte

*Controlul formatului* – se referă la fișierele text care sunt transferate direct către o imprimantă:

*Structura*

*Modul de transmitere* care poate fi:

- Stream – fișierul este transferat într-o serie de bytes
- Bloc – fișierul este transferat bloc cu bloc, fiecare cu un header
- Comprimat – se folosește o schemă de comprimare a secvențelor de bytes identici.

În timpul unui transfer prin ftp nu există nici un mecanism de negociere a transmisiei.

## **MAIL(POȘTA ELECTRONICĂ)**

Toate programele specializate în poșta electronică funcționează pe baza unor protocoale de comunicație. SMTP(Simple Mail transport Protocol) – Protocolul de transport simplu de e-mail – oferă servicii de transmitere de mesaje peste TCP/IP și suportă majoritatea programelor de e-mail de pe Internet.

SMTP este un protocol folosit pentru a transmite un mesaj electronic de la un client la un server de poștă electronică. După stabilirea conexiunii TCP la portul 25 (utilizat de SMTP), calculatorul-sursă(client) așteaptă un semnal de la calculatorul-receptor (server). Serverul începe să emită semnale declarându-și identitatea și anunțând dacă este pregătit sau nu să primească mesajul. Dacă nu este pregătit, clientul părăsește conexiunea și încearcă din nou, mai târziu. Dacă serverul este pregătit să accepte mesajul, clientul anunță care este expeditorul mesajului și care este destinatarul. Dacă adresa destinatarului este validă, serverul dă permisiunea de transmitere a mesajului. Imediat clientul îl trimite, iar serverul îl primește. După ce mesajul a fost transmis, conexiunea se închide. Pentru ca un client al serviciului de poștă electronică să primească un mesaj de la serverul specializat în aceste tipuri de servicii, apelează fie la Post Office Protocol (POP), fie la Internet Message Access Protocol (IMAP) Spre deosebire de POP(mai vechi) care presupune că utilizatorul își va goli cutia poștală pe calculatorul personal la fiecare conectare și va lucra deconectat de la rețea (off-line) după aceea, IMAP păstrează pe serverul de e-mail un depozit central de mesaje care poate fi accesat on-line de utilizator de pe orice calculator.

**Protocolul DHCP (Dynamic Host Configuration Protocol)** are scopul de a permite calculatoarelor dintr-o rețea să obțină automat o adresă IP, printr-o cerere către serverul DHCP. Serverul poate să furnizeze stației respective toate informațiile de configurare necesare, inclusiv adresa IP, masca de subrețea, default gateway, adresa serverului DNS, etc.

Astfel, când serverul primește o cerere de la o stație, selectează adresa IP și un set de informații asociate dintr-o mulțime de adrese predefinite care sunt păstrate într-o bază de date. Odată ce adresa IP este selectată, serverul DHCP oferă aceste valori stației care a efectuat cererea. Dacă stația acceptă oferta, serverul DHCP îi împrumută adresa IP pentru o perioadă, după care o regenerează.

Generarea adreselor IP prin serverul DHCP este o metodă utilizată pe scară largă în administrarea rețelelor de mari dimensiuni. Folosirea unui server DHCP simplifică administrarea unei rețele pentru că software-ul ține evidența adreselor IP. În plus, este exclusă posibilitatea de a atribui adrese IP invalide sau duplicate.

**Protocolul SNMP(Simple Network Manage Protocol)** –permite administratorilor de rețea gestionarea performanțelor unei rețele, identificarea și rezolvarea problemelor care apar, precum și planificarea dezvoltărilor ulterioare ale rețelei.

SNMP are trei componente de bază:

- *Stațiile de administrare (Network Management Station)* - pot fi oricare din calculatoarele rețelei pe care se execută programele de administrare
- *Agenții* - dispozitivele administrate
- *Informațiile de administrare ( Management Information Base)* – colecție de date organizate ierarhic care asigură dialogul dintre stația de administrare și agenți